UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. EVGENI KOPANKOV, Defendant.	Case No. 19-cr-00178-JSC-1 **ORDER FOLLOWING PRETRIAL CONFERENCE NO. 2**

After conducting a pretrial conference on May 10, 2023, the Court orders as follows:

I. THE CELL PHONE DATA IS EXCLUDED.

A. Background

On May 5, 2023, the government advised the Court and Defendant that "on May 3, 2023, counsel for the United States learned that an examiner was able to unlock the phone seized from defendant Evegeni Kopankov during his April 2019 arrest." (Dkt. No. 292 at 1.)[1] Defendant argues the evidence obtained is inadmissible because the government searched the phone without a warrant. The Court agrees.

1. The First Warrant

Magistrate Judge Illman approved a warrant for the device when it was seized on April 9, 2019. (Dkt. No. 296-1 at 2; *see also* No. 1:19-MJ-70519-RMI.) The warrant authorized the search of "A white iPhone X, containing Verizon SIM Card: 8914800000463126909 2 seized from Evgeni Kopankov on April 3, 2019."[2] (*Id.*)

The warrant contained an addendum known as "Attachment C." (Dkt. No. 304-1 at 32.)

[1] Record citations are to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of the documents.

[2] While the parties have not raised the issue, it appears Defendant's device was in fact an iPhone "XS" rather than an iPhone "X" as described in the warrant. (Dkt. No. 292-2 at 1.)

Attachment C provides a "Protocol For Searching Devices or Media that Store Data Electronically." (*Id.*) Relevant here, Attachment C states:

> 1. In executing this warrant, the government will begin by ascertaining whether all or part of a search of a device or media that stores data electronically ("the device") reasonably can be completed at the location listed in the warrant ("the site") within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if removal is necessary to preserve evidence, or if the item is contraband, a forfeitable instrumentality of the crime, or the fruit of a crime.
>
> 2. If the government determines that a search reasonably cannot be completed on site within a reasonable time period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then conducting the forensic review of the mirror image or duplication off site. The government will complete a forensic review of that mirror image within 120 days of the execution of the search warrant.
>
> 3. In a circumstance where the government determines that a mirror image of the contents of a device cannot be created on site in a reasonable time, the government may seize and retain that device for 60 days in order to make a mirror image of the contents of the device.
>
> [. . .]
>
> 5. When the government removes a device or related equipment or documents from the site in order to create a mirror image of the device's contents or to conduct an off-site forensic review of the device, the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents within 14 calendar days of the execution of the search warrant.
>
> […]
>
> 7. The time periods set forth in this protocol may be extended by court order for good cause.

(*Id.* at 31-32.) In the warrant application, an agent affirmed he was "familiar with the protocol set forth in Attachment C and [would] abide by the requirements." (Dkt. No. 304-1 at 21.)

2. Unlocking the Device

The government first sent the device to the Silicon Valley Regional Computer Forensics Laboratory. (Dkt. No. 296-1 at 2 ¶ 7.) That lab was unable to unlock the device. (*Id.* ¶ 8.) The device was then sent to Quantico, Virginia. (*Id.* ¶ 11.) Two FBI units then began a "brute force"

attack to obtain Defendant's passcode on April 30, 2020. (*Id.* ¶¶ 12, 14.) Put differently, the FBI used an automated software program to guess the correct password. (*See* Dkt. No. 304-4.)

The "brute force" process entailed the following steps. The device was plugged into a computer. (Dkt. No. 304-4 ¶ 8.) The computer installed software onto the device. (*Id.* ¶ 8.) The device was unplugged from the computer. (*Id.*) The software "automates the brute forcing process" so long as the device is connected to a charging cable. (*Id.* ¶¶ 9-10.) The process is lengthy. A six-digit passcode can be any one of up to 1,000,000 combinations and iPhones contain software that pause guessing attempts after a certain number of incorrect entries. (Dkt. No. 304-5 ¶¶ 24-28.) The government represents it "is not uncommon for entire racks of phones to be undergoing brute force attacks for years." (Dkt. No. 304-4 ¶ 11.)

Because Attachment C imposed a time limit for the government to "make a mirror image of the contents of the device," in March 2021, the government requested an extension until June 20, 2021 to access the device.[3] (Dkt. No. 304-1 at 35-37.) That extension, if granted, would have expired on June 20, 2021. (Dkt. No. 296-1 at 3 ¶ 15.) But the "brute force" attack appears to have continuously operated from at least June 17, 2020, until the password was discovered on May 2, 2023. (Dkt. No. 304-5 ¶ 12.)

3. Accessing the Device

The FBI Digital Forensic Examiner learned the passcode on May 2, 2023. (Dkt. No. 304-5 ¶ 31.) He then obtained "a full file system extraction" via a "GrayKey device." (*Id.* ¶ 32.) The examiner states: "I accomplished this by unlocking the device, using the passcode, on May 2. I physically took the device, unlocked the device using the passcode, and plugged it into a GrayKey device (which resembles a small box), using the DEVICE's 'lightening' port." (*Id.* ¶ 33.) After the examiner manually entered the passcode, the GrayKey device extracted the contents of the

[3] The government has not submitted any evidence Judge Illman ever, in fact, granted this extension request to extend the mirroring time to June 2021. Rather, the sole evidence the government provides is Agent Soli's March 2021 declaration requesting the extension. (*See* Dkt No. 304-1 at 35-37; *compare* Case No. 3:23-mj-70619-LB, Dkt. No. 1 at 3 ¶ 15 (indicating a signed extension order was attached) *with* Dkt. No. 2 at 19-21 (Agent Soli's affidavit requesting an extension, not a signed order).) Review of the underlying docket does not show the extension was requested or granted. (*See* Case No. 1:19-MJ-70519-RMI, Dkt. No. 1.)

device. (*Id.* ¶ 34.) The Examiner then copied that data onto a USB drive. (*Id.* ¶ 32.) But the examiner states he "did not view any of the contents" on the device. (*Id.* ¶ 35.) He did, however, create a technical report, regarding the phone's contents which he submitted (with the extraction data) to the Silicon Valley Regional Computer Forensics Laboratory. (*Id.* ¶¶ 36, 40.)

The GrayKey report indicates the system extracted 22.69 gigabytes of data, including "109 Keys, 12 Certificates, 83 Internet passwords, 429 General passwords." (Dkt. No. 292-2 at 2.) The report lists the "Owner Name" as "Evgeni Kopankov" and under "Accounts" the readout lists "ekopankov@gmail.com." (*Id.* at 1.)

4. The Second Warrant

On May 4, 2023, after the government unlocked the phone and extracted its contents via the GrayKey device, the government requested a renewed search warrant for the device. (*See* Case No. 3:23-mj-70619-LB.) The affiant requesting the new warrant explained "the examiner has, or will soon, mail the phone back to evidence at the FBI's office at 450 Golden Gate Avenue in San Francisco and provide investigators with an electronic copy of the contents of the phone." (Dkt. No. 296-1 at 4 ¶ 26.) The government requested a warrant "to examine the contents of the phone." (*Id.* ¶ 28.)

B. Analysis

The government concedes it violated Attachment C by "creating a mirror" of the phones' contents after the period to do so had elapsed. (Dkt. No. 304 at 8.) Nevertheless, the government contends the evidence gained during that process is admissible. The Court disagrees.

1. A Fourth Amendment violation occurred.

The Fourth Amendment protects people from "unreasonable searches and seizures" of "their persons, houses, papers, and effects." U.S. Const. amend. IV. The default rule is that a search or seizure is unreasonable unless conducted pursuant to a warrant. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995).

The government generally may not search a cell phone without a valid search warrant. *Riley v. California*, 573 U.S. 373, 386 (2014). As the Supreme Court explained in *Riley*:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life[.]" The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

Id. at 403 (citations omitted). The government got a warrant. But it expired. The government concedes it violated Attachment C by mirroring the device after the time to do so expired. But it argues that mirroring was not a "search" and did not require a valid search warrant.

The GrayKey extraction was a search and seizure because the government physically invaded Defendant's phone to gain information without a valid warrant. In *United States v. Dixon*, 984 F.3d 814, 820 (9th Cir. 2020), the Ninth Circuit held physical intrusion into a constitutionally protected space is a search when done to gain information. As *Dixon* explains:

> When Officer Ochoa inserted the key into the minivan's lock, an "effect," he physically intruded onto a constitutionally protected area. This physical intrusion was done for the express purpose of obtaining information, specifically to learn whether Dixon exercised control over the minivan. Thus, the insertion of the key into the minivan's lock constituted a search within the meaning of the Fourth Amendment.

Here, the same principles apply. The examiner declared he "physically took the device, unlocked the device using the passcode, and plugged it into a GrayKey device (which resembles a small box), using the DEVICE's 'lightening' port." (Dkt. No. 304-5 ¶ 33.) And he did so to download the contents of Defendant's phone onto a USB drive. (*Id.* ¶ 32.) Put differently, that physical invasion into Defendant's constitutionally protected device downloaded "the privacies" of Defendant's life. *Riley*, 573 U.S. at 403. That physical invasion constitutes a search. *Cf. United States v. Sam*, No. CR19-0115-JCC, 2020 WL 2705415, at *2 (W.D. Wash. May 18, 2020) (powering on a phone to take a photo of the phone's lock screen constituted a physical search).

The government's contrary arguments are unpersuasive. First, the government argues the government did not "search" the phone because the examiner merely duplicated the contents of the phone rather than reviewing them. Not so. Even absent human review of the files within the phone, the GrayKey report—which the examiner sent to multiple government agents—includes personal information such as the size of the phone's contents and a specific number of internet

passwords therein. And, just as inserting the key into the minivan lock established vehicle ownership in *Dixon*, the insertion of the GrayKey device into the phone helped the government establish Defendant's ownership over the device here. Prior to the GrayKey report, the government knew only that Kopankov was arrested with the phone. Now, after inserting a cable into the device, the GrayKey report indicates Kopankov owns the phone and his email address is associated with the device. Thus, just as the physical invasion in *Dixon* yielded information, so too did the physical invasion here. So, even without reviewing the contents of the phone in depth, the GrayKey insertion still revealed to the government certain privacies regarding the phone before the government re-obtained a valid warrant. This was a search.

The government's citation to *United States v. Carrington*, 700 F. App'x 224, 232 (4th Cir. 2017) is inapposite. In *Carrington*, the Fourth Circuit found the warrant did not limit the time for the government to complete the forensic review of the device. *Id.* The court concluded Federal Rule of Criminal Procedure 41(e)'s 14-day limitation governs only time for seizure or on-site copying of media or information, not later off-cite copying or review. *Id.* But here, unlike the warrant in *Carrington*, Attachment C set explicit time limits on when the government could mirror the device. (Dkt. No. 304-1 at 32.) Rule 41 does not limit a judge's ability to add restrictions to guide search warrant execution. *See* Fed. Crim. P. 41(e)(2)(B), 2009 Advisory Comm. Notes ("The rule does not prevent a judge from imposing a deadline for the return of storage media or access to the electronically stored information at the time the warrant is issued"). Attachment C set such limits here. The government promised to abide by those requirements during the search. But the government admits the examiner did not follow those limits. So, unlike in *Carrington*, here the government was not operating pursuant to a valid warrant.

The government next argues the existence of probable cause means there was no need for a warrant. The government states:

> Strict adherence to Attachment C is of the highest importance, but a warrantless search devoid of probable cause—the reason the search was unconstitutional in *Dixon*—is an error of a very different magnitude than the creation of a mirror image in violation of Attachment C, two days before a new warrant is obtained. Here, the government had probable cause to search the phone.

(Dkt. No. 304 at 7.) A small constitutional violation is no less a constitutional violation. Indeed, "two days before a new warrant is obtained" is just a creative way to say, "almost two years after the original warrant expired." The government admits it did not search the phone pursuant to a valid warrant. The excuse that the examiner did not need a warrant because he had probable cause is wrong. *See United States v. Young*, 573 F.3d 711, 722 (9th Cir. 2009) ("What is missing from this kind of circular logic is the fact that the police officer could have obtained a warrant[.]")

In sum, the search here violated Defendant's rights under the Fourth Amendment.[4]

2. Exclusion is warranted.

The exclusionary rule—"a prudential doctrine created by th[e] [Supreme] Court to compel respect for the constitutional guaranty" of the Fourth Amendment, *Davis v. United States*, 564 U.S. 229, 236 (2011) (cleaned up)—is "applicable only . . . where its deterrence benefits outweigh its substantial social costs," *Hudson v. Michigan*, 547 U.S. 586, 591 (2006) (cleaned up). The rule is therefore subject to certain well-established exceptions. The government argues the Court should apply the independent source exception or, alternatively, the good faith exception to the exclusionary rule. Neither exception applies.

a. Independent Source

Under the independent source exception, suppression is unwarranted when unlawfully obtained evidence is "later obtained independently from activities untainted by the initial illegality." *United States v. Saelee*, 51 F.4th 327, 335 (9th Cir. 2022) (quoting *Murray v. United States*, 487 U.S. 533, 537 (1988)). To establish "evidence initially acquired unlawfully" has later been independently obtained through an untainted source, the government must show "that no information gained" from the Fourth Amendment violations "affected either [1] the law enforcement officers' decision to seek a warrant or [2] the magistrate's decision to grant it." *Id.*

[4] The government had not yet filed its expert declarations explaining the difference between the brute force method and the GrayKey method when Defendant filed this motion. Thus, Defendant's motion to suppress focuses on the government's physical invasion using the GrayKey device, rather than the "brute force" attempts outside the warrant period. The Court's holding—that the physical invasion was a search—does not mean the "brute force" attack on the phone was not a search. Rather, the Court does not address that "brute force" issue because it was not raised in the initial motion.

The government has not met its burden regarding "the law enforcement officers' decision to seek a warrant." *Id.* As stated in the affidavit, the government sought the warrant to review the device's contents only *after* the GrayKey device performed the extraction. (Dkt. No. 296-1 ¶ 26-28.) That GrayKey report, as discussed above, confirmed for the government that Kopankov owned the phone, that the phone was associated with his email account, and that the phone had a great deal of information within it. In other words, the government only knew the scope of the "contents" it wished to search after it had already searched the phone without a warrant.

The government provides no contrary evidence. The independent source doctrine asks, "whether the evidence *actually* was 'obtained independently from activities untainted by the initial illegality,'" not whether evidence "would have" been discovered by lawful means absent the illegal search. *United States v. Lundin*, 817 F.3d 1151, 1161 (9th Cir. 2016) (quoting *Murray*, 487 U.S. at 537) (emphasis in original). The facts of *Saelee* show when an independent source exception is appropriate. There, the government showed it had prepared a near-complete warrant application (save one paragraph) before the unconstitutional search. *Saelee*, 51 F.4th at 335-336. The warrant was completed "minutes" after the allegedly illegal arrest and entry and "*before* most (if not all) the ensuing search and seizure activities." *Id.* at 336 (emphasis added). This is the opposite scenario. In a lab across the country, a government technician—operating without a warrant—physically entered the device and extracted its data. The examiner generated a report with personal information and forwarded that report to other government agents. Only then, days (not minutes) later, did the government seek a warrant. Thus, *Saelee*'s facts are distinguishable here.

The examiner effectively stood on Defendant's doorstep and tried fitting different keys into his front door lock for years after the warrant expired. Then, when the door finally opened, the government entered the threshold and seized the information therein and reviewed some (but admittedly not all) of it. Now the government asks to excuse this unlawful entry because the government "had been hoping for the phone to be accessed for years." (Dkt. No. 304 at 8.) Maybe so. But they only got a warrant *after* the illegal search yielded the information they hoped for. Put differently, if the government's conduct were excused here, Attachment C, which was

expressly part of the warrant, would become a nullity because its carefully calculated time limits would be meaninglesss.

b. Good Faith Exception

The government's good faith argument is similarly unpersuasive.[5] The government knew it needed to obtain a warrant extension to comply with Attachment C. Indeed, it claims it did so once. But it failed to do so here. The government cites no declaration to support its statement that "the examiner. . . was relying on a search warrant signed by a magistrate judge." (Dkt. No. 304 at 9.) Indeed, the examiner's declaration does not even contain the word warrant. (Dkt. No. 304-5.) So, the government knew it needed a warrant. But it only sought one after the search had occurred.

That troubling omission justifies exclusion to deter such deliberate indifference to Fourth Amendment rights in the future. The government claims this situation is unlikely to reoccur. But the evidence is to the contrary. The government's declarations describe "entire racks of phones" undergoing "brute force attacks for years." (Dkt. No. 304-4 ¶ 11.) So this not only can, but will happen again unless the government ensures it has a valid—and generally required—warrant to peer inside those phones. *Riley v. California*, 573 U.S. 373, 386 (2014). Exclusion here will ensure greater care is taken with such devices and ensure compliance with "the protection for which the Founders fought." *Id.* at 403.

* * *

In sum, a Fourth Amendment violation occurred—at a minimum—when the government seized and searched the cell phone's contents with the GrayKey tool and generated the GrayKey report.[6] And, because no exception to the exclusionary rule applies, suppression is warranted.

II. THE CO-CONSPIRATOR STATEMENT AUTHENTICATION PROFFER

The government intends to authenticate the various recordings at issue in this case through

[5] For the reasons discussed in part I.B.1, the Court rejects the government's fourth argument that the violation of Attachment C was a technical error rather than a constitutional violation. (Dkt. No. 304 at 8.)

[6] The Court need not address Plaintiff's alternative theory that the warrant was insufficient under *Franks v. Delaware*, 438 U.S. 154 (1978).

Agent Williamson's testimony. As discussed at the pretrial conference, the government shall provide a proffer as to the authenticity of the recordings on Monday, May 15, 2023 after jury selection.

III. COMPELLED IMMUNITY FOR THE CHS

Defendant moves to compel the government to grant use immunity to a defense witness—Ilija Ristik. To compel the government to grant immunity, defendant must show:

> (1) the defense witness's testimony was relevant; and
>
> (2) either (a) the prosecution intentionally caused the defense witness to invoke the Fifth Amendment right against self-incrimination with the purpose of distorting the fact-finding process; or
>
> (b) the prosecution granted immunity to a government witness in order to obtain that witness's testimony, but denied immunity to a defense witness whose testimony would have directly contradicted that of the government witness, with the effect of so distorting the fact-finding process that the defendant was denied his due process right to a fundamentally fair trial.

United States v. Wilkes, 744 F.3d 1101, 1105 (9th Cir. 2014) (quoting *United States v. Straub*, 538 F.3d 1147, 1162 (9th Cir. 2008)).

The first factor is met. Ristik's testimony is relevant given he made recordings at issue in this case and was a witness to a number of the events during the alleged conspiracy.

The second factor, however, is not satisfied. At this stage, the Court understands Defendant as only making an argument for immunity under prong 2(b)—not prong 2(a) of the *Straub* test. To satisfy prong 2(b), Defendant must show the government offered immunity to a government witness but denied immunity to a defense witness whose testimony would have "*directly contradicted*" that of "*the* government witness" granted immunity. *Straub*, 538 F.3d at 1162 (emphasis added).

The first section of prong 2(b) is met. The government has offered immunity (or plea bargains) to various witnesses in this case—namely Borisov and Brooks. *See Wilkes*, 744 F.3d at 1105 n.1 (9th Cir. 2014) ("Our cases make clear that government witnesses who are granted favorable plea deals in return for their testimony are encompassed by *Straub* use of the term 'immunized'"); *United States v. Young*, 86 F.3d 944, 948 (9th Cir. 1996) (same). And the

government is unwilling to offer a potential defense witness—Ristik—immunity. (Dkt. No. 298.)

But, at this stage, Defendant's proffer does not explain how Ristik will offer testimony that "directly contradict[s]" the testimony of Brooks or Borisov. *Wilkes*, 744 F.3d at 1105. "[A] witness directly contradicts another witness if their respective testimonies cannot simultaneously be true, although in this context the proffered defense testimony 'need only support (as opposed to compel) a finding by the jury that it was 'directly contradictory.'" *Id.* (citing *Straub*, 538 F.3d at 1163). The defense argues:

> Mr. Ristik's testimony can impeach Mr. Brooks' testimony and the government's narrative that Brooks and Borisov committed overt acts largely on the belief that "Kopankov was going to provide the information about the timing and whereabouts of the arrival of the money to be robbed and the target to be kidnapped—evidently, a man named "Sergey," who was then in Las Vegas—and provide guns to do so." Dkt. 263 at 4. Mr. Ristik will testify that he chose and paid for the airline tickets and clothing allegedly used by Mr. Borisov and Mr. Brooks and paid Mr. Borisov $1000 to ensure he would agree to go to California. Gov't Ex. 132 at 35:57-37:38; Exhibit B, EK-78. He will testify that he suggested many aspects of the alleged robbery, wowing Mr. Borisov by telling him that the alleged target had buried $150 million. Gov't Ex. 001, 13:52-24:15 (Ristik: "I even (Ivan), I even (Ivan)—you know who is this guy? This guy was with Olympics. And I keep hearing about this guy. They say they got $150 million dollars buried in there"). The jury must be allowed to see and hear Mr. Ristik and the degree to which he directed the alleged plot in this case, and why.

(Dkt. No. 308 at 5.) Without knowing what testimony Brooks or Borisov will provide, the Court cannot determine whether the above statements are irreconcilable with that testimony such that both cannot be simultaneously true.

Defendant's motion to compel immunity is accordingly denied without prejudice.

IV. RULE 410 DOES NOT BAR THE PRESENTENCE REPORT FOR REBUTTAL OR IMPEACHMENT.

As discussed at the pretrial conference, Federal Rule of Evidence 410 does not cover any statements Kopankov made to the probation officer during the preparation of the presentence report. *See United States v. Chisholm*, No. 2:14-CR-132, 2015 WL 13309388, at *4 (E.D. Va. July 31, 2015); *United States v. Jim*, 839 F. Supp. 2d 1157, 1187 (D.N.M. 2012), *aff'd*, 786 F.3d 802 (10th Cir. 2015). However, because that report is not on the Government's exhibit list, it is

admissible only for purposes of impeachment or rebuttal.

V. HENTHORN QUESTIONING

As discussed at the pretrial conference, Defendant has made a showing that FBI Special Agent Michael Mangan's past interactions with confidential human sources, and particularly the confidential source relevant in this matter, will be relevant here. The government may object to particular questions at trial should Agent Mangan testify.

VI. THE JOINT CASE STATEMENT

As discussed at the pretrial conference, the parties are to submit a joint case statement to be read to the jury prior to voir dire by May 11, 2023.

VII. THE JURY INSTRUCTIONS

The parties shall provide updated proposed jury instructions on or before May 12, 2023.

VIII. UPDATED WITNESS AND EXHIBIT LISTS

The parties shall file updated witness and exhibit lists by May 12, 2023.

IX. CONTEMPT PROCEEDINGS

The government's submission regarding remedies for Mr. Borisov's anticipated contempt shall be filed by May 12, 2023.

X. TRIAL SCHEDULE

As previously discussed, the Court anticipates the trial schedule will be as follows:

Monday, May 15, 2023:	8:30 a.m. for jury selection and recording authentication
Tuesday, May 16, 2023:	8:30 a.m. to 3:00 p.m.
Wednesday, May 17, 2023:	8:30 a.m. to 3:00 p.m.
Thursday, May 18, 2023:	8:30 a.m. to 1:30 p.m. (no lunch break)
Friday, May 19, 2023:	No trial
Monday, May 22, 2023:	8:30 a.m. to 3:00 p.m.
Tuesday, May 23, 2023:	8:30 a.m. to 3:00 p.m.
Wednesday, May 24, 2023:	8:30 a.m. to 3:00 p.m.
Thursday, May 25, 2023:	8:30 a.m. to 1:30 p.m. (no lunch) (unless jury deliberating)

The Court will advise the venir that the parties intend for them to get the case the week of

May 22, but that we want to confirm that all are available through May 31, 2023.

IT IS SO ORDERED.

This Order resolves Dkt. No. 296

Dated: May 11, 2023

JACQUELINE SCOTT CORLEY
United States District Judge

United States District Court
Northern District of California